

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
NORTHERN DIVISION**

STEVEN NELSON ELLER
1159 Hammonds Plains Dr.
Crownsville, MD 21032
Anne Arundel County

Plaintiff,

v.

DEFENDANT “1” a/k/a “Laura Mayer” and JOHN DOE Defendants 1-9 who are the cohorts of Defendant “1” and are the owners of the following cryptocurrency deposit wallets where Plaintiff’s stolen cryptocurrency assets were transferred:

Binance:

0xce76ae7911bf900b761f623137e3d4a4a483a5fc,
0xe40650e151115032699dd0a32b8112c4c41f1448,
0xc6cefb645bb13d9b79e4b2e5e3ef657143e7162,
0x7097f6377d7be6a3be7999f13f75a20d98eae982, and
0x9a163b2601d931c6e07b91473d6b8ea1a5cac5c9

Remitano:

0x7407d51f0cc58350bfbe96f208a4dc2cc8a85e7e and
0xb23297bc22e7de35238b4fe003f37973bb038afc

Btse.com:

0x5974827c4e0a641fd15543fefceb634608e78b35

HTX:

0x8552681ca9fdb2be3b383c4fd0e90b3789609253

Defendants.

Complaint for a Civil Case

Case No. _____

JURY TRIAL DEMAND

**COMPLAINT FOR
VIOLATION OF THE RACKETEER INFLUENCED
AND CORRUPT ORGANIZATIONS ACT**

Plaintiff, STEVEN NELSON ELLER, by and through undersigned counsel, sues
DEFENDANT “1” a/k/a “Laura Mayer” and JOHN DOE Defendants 1-9, as follows:

PRELIMINARY STATEMENT

1. Defendants stole 132.38456 Ethereum (ETH), 2.83406 Bitcoin (BTC), and 198,704.02691 Tether (USDT) from Plaintiff pursuant to a sophisticated global internet cryptocurrency fraud and conversion scheme, the current market value of which is eight hundred thirty-one thousand five hundred dollars and seventy-six cents (\$831,500.76)¹.

2. Defendant “1” played a material role in the theft of Plaintiff’s assets, and upon information and belief, she and her cohorts currently possess all or a significant portion of Plaintiff’s stolen property.

3. Plaintiff brings this lawsuit to recover his stolen assets.

SUBJECT MATTER JURISDICTION AND VENUE

4. This is an action for damages related to the theft of Plaintiff’s cryptocurrency assets as detailed below. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 (diversity jurisdiction). This action includes damages pursuant to 18 U.S.C. § 1964 (the “Racketeer Influenced and Corrupt Organizations Act” or “RICO”). This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 (federal question).

5. Venue is proper in this District pursuant to 18 U.S.C. § 1965(a) and (b), and 28 U.S.C. § 1391(b) and (c).

6. Defendants are subject to personal jurisdiction in this district, because they direct business activities toward and conduct business with consumers throughout the United States, including within the State of Maryland and this district through at least a fraudulent website and mobile application (Bitfract-pro.net) which can be accessed on the internet and on smartphones and are accessible from Maryland.

¹ Current market value calculated using data from etherscan.io and blockchain.com on July 18, 2024.

7. Plaintiff accessed the fraudulent website and mobile application (Bitfract-pro.net) in the State of Maryland and the theft occurred while Plaintiff was located in the State of Maryland. Defendants directed numerous false and fraudulent representations to Plaintiff in this district, stole Plaintiff's assets within this district, and caused significant harm to Plaintiff in this district.

8. Moreover, Defendants are foreign nationals and are subject to personal jurisdiction in this district pursuant to Federal Rule of Civil Procedure 4(k)(2) because (i) Defendants are not subject to jurisdiction in any state's court of general jurisdiction; and (ii) exercising jurisdiction is consistent with the United States Constitution and laws.

THE PARTIES AND PERSONAL JURISDICTION

9. Plaintiff, STEVEN NELSON ELLER, an individual, is *sui juris*, and is a resident and citizen of Maryland.

10. Defendant "1" is an individual, is *sui juris*, and is subject to the personal jurisdiction of this Court. Defendant "1" represented to Plaintiff Steven Nelson Eller that her name was "Laura Mayer". Defendant represented to Plaintiff that she was originally from Germany but currently living in Los Angeles, California. The parties' communications consistently demonstrated Defendant "1" was of German descent; however, based off of bank wire information provided by Defendants, Defendant "1" is likely located in Hong Kong.

11. JOHN DOE Defendants 1-9 are the cohorts of Defendant "1" and are the owners of the following cryptocurrency deposit wallets where Plaintiff's stolen cryptocurrency assets were transferred:

- Binance:
 - 0xce76ae7911bf900b761f623137e3d4a4a483a5fc
 - 0xe40650e151115032699dd0a32b8112c4c41f1448
 - 0xc6cefbb645bb13d9b79e4b2e5e3ef657143e7162
 - 0x7097f6377d7be6a3be7999f13f75a20d98eae982

- 0x9a163b2601d931c6e07b91473d6b8ea1a5cac5c9
- Remitano:
 - 0x7407d51f0cc58350bfbe96f208a4dc2cc8a85e7e
 - 0xb23297bc22e7de35238b4fe003f37973bb038afc
- Btse.com:
 - 0x5974827c4e0a641fd15543fefceb634608e78b35
- HTX:
 - 0x8552681ca9fdb2be3b383c4fd0e90b3789609253

12. JOHN DOE Defendants 1-9 are *sui juris* and subject to the personal jurisdiction of this court. JOHN DOE Defendants 1-9 have intentionally concealed their identity as part of their scheme to defraud Plaintiff, but as part of their conspiracy directed fraudulent communications towards Plaintiff in Maryland, causing Plaintiff to suffer significant economic and emotional harm while in Maryland.

13. At all times material hereto, Defendants have maintained and continue to maintain private cryptocurrency wallets and cryptocurrency exchange accounts in which all of or a portion of Plaintiff's stolen cryptocurrency currently sits.

ALLEGATIONS COMMON TO ALL COUNTS

A. Defendants Execute an International Cryptocurrency Theft Scheme

14. Plaintiff is a victim of not only a nationwide but also a worldwide RICO conspiracy known as "pig butchering."

15. Pig butchering scams are "fraudulent crypto investment schemes directed from Asia," which are now a billion-dollar industry.²

16. Pig butchering scams run and perpetrated by organized criminal groups in Southeast Asia, are called such because the victims are "likened to hogs fattened up for slaughter."³

² <https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/>

³ <https://www.nbcnews.com/news/crime-courts/pig-butchering-scams-rise-fbi-moves-stop-bleeding-rcna137009>

17. The scammers, typically located in Southeast Asia, carefully research their victims, and can spend months grooming the victim to gain their trust.

18. Pig butchering scammers utilize expertly crafted copycat websites that replicate authentic trading platforms. These scammers simulate trades and returns and the victims are unaware of the scheme.⁴

19. The perpetrators of these so-called pig butchering scams befriend victims and over time build up trust. Once that trust is gained, the perpetrators claim to be experts in cryptocurrency investments, fraudulently represent themselves to be experts in cryptocurrency investing, and convince victims to send their digital assets to fake copycat exchanges.

20. Plaintiff had no experience trading cryptocurrency prior to being approached by Defendant “1” a/k/a “Laura Mayer”.

21. On or about February 15, 2023, Plaintiff was approached by Defendant “1” a/k/a “Laura Mayer” who communicated with Plaintiff via LinkedIn, and later via Telegram, with a Telegram phone number of 213-478-9474 (VOIP).

22. Defendant “1” misrepresented that she would teach Plaintiff how to become a successful cryptocurrency trader.

23. Defendant “1” lured Plaintiff by showing him examples over Telegram of how she was successfully earning high returns on her cryptocurrency trading methods.

24. Defendant “1” represented to Plaintiff that she was using a trusted trading platform called Bitfract-pro.net.

25. Defendant “1” assisted Plaintiff in downloading and accessing Defi Wallet and then transferring cryptocurrency to Bitfract-pro.net which she claimed was a legitimate decentralized

⁴ <https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/>

trading exchange that could only be accessed through Defi Wallet. She stated that “Bitfract-pro.net” would be used as a trading platform with the purpose of making transactions; and when done, the assets would be transferred to Plaintiff’s wallet for withdrawal.

26. However, the application Defendant “1” provided to Plaintiff was not a legitimate exchange website owned and operated by any exchange but was instead a fraudulent website created to deceive individuals, including Plaintiff, into believing they were investing on a legitimate cryptocurrency exchange.

27. To further entice Plaintiff into believing she was a legitimate investor who only wanted to assist Plaintiff in becoming a successful cryptocurrency trader like her, on or about May 3, 2023, Defendant “1” had Plaintiff run a test where he transferred approximately \$1,000 worth of cryptocurrency from his Defi account into the fraudulent Bitfract-pro.net platform. When Plaintiff was able to transfer this amount back to his digital wallet, he believed that Defendant “1” was a legitimate investor who wanted to help him learn how to invest cryptocurrency and, further, that the fraudulent website he had accessed was also legitimate.

28. After familiarizing himself with the process of trading on the fraudulent mobile application recommended by Defendant “1,” and in reliance on the foregoing false and fraudulent misrepresentations, Plaintiff started to transfer cryptocurrency from his Coinbase and OKCoin account, legitimate third-party online platforms for buying, selling, transferring, and storing cryptocurrency, to Defi Wallet and then eventually into the fraudulent platform.

29. Defendants posted fraudulent returns on their fake website which made it appear that Plaintiff was making money on his trades. As a result, he continued to transfer cryptocurrency from his Coinbase and OKCoin accounts to the fraudulent exchange.

30. Because of the fraudulent representations contained on the fake Bitfract-pro.net

platform, and misrepresentations made by Defendant “1”, Plaintiff believed that he had made significant money from his previous investments.

31. Plaintiff was told by Defendant “1” that the value of his cryptocurrency had grown significantly, which was reflected on the fraudulent Bitfract-pro.net statements.

32. Plaintiff was happy with what he believed was a significant return on Plaintiff’s investment. However, when Plaintiff decided it was time to transfer all the cryptocurrency from Bitfract-pro.net back to Plaintiff’s Coinbase and OKCoin accounts, he discovered that his funds has been frozen.

33. Plaintiff attempted to reach what he thought was BitFract-pro help desk for five days to get an explanation on why his funds had been frozen. Eventually, Plaintiff received a response from “BitFract-pro help desk” stating that Plaintiff’s account had been suspected of money laundering, tax evasion, or other criminal activity and had been suspended in accordance with U.S. Federal regulations. In addition, Plaintiff would be required to post a one hundred thousand dollar (\$100,000.00) bond within ten business days.

34. This is when Plaintiff realized he had been scammed. Plaintiff refused to pay the additional one hundred thousand dollars (\$100,000.00) and made numerous unsuccessful attempts to transfer the cryptocurrency from the fake exchange back to his Coinbase and OKCoin wallets.

B. Plaintiff’s Forensic Tracing of His Stolen Cryptocurrency

35. When a transaction is made on the blockchain it is assigned a “transaction hash” (“TXID”). A transaction hash is a unique string of characters that is given to every transaction that is verified and added to the blockchain. A TXID is used to uniquely identify a particular transaction. All on-chain transactions (the transactions from or to external addresses) have a unique TXID that can be seen in transaction details. All on-chain transactions (depositing and

withdrawing of funds) have a unique TXID that can be found in transaction details.

36. Within the time frame of April 26, 2023 and June 25, 2023, Plaintiff STEVEN NELSON ELLER made 5 transactions from his Coinbase and OKCoin accounts to Defi Wallet and then to the fraudulent exchange. In total, Plaintiff transferred approximately 132.38456 Ethereum (ETH), 2.83406 Bitcoin (BTC), and 198,704.02691 Tether (USDT) to the fraudulent exchange, which has a current market value of eight hundred thirty-one thousand five hundred dollars and seventy-six cents (\$831,500.76).

37. Plaintiff has retained forensic cryptocurrency tracing experts who have traced Plaintiffs stolen assets on the blockchain. Attached hereto as Exhibit “1” is the tracing report completed by experts at CNC Intelligence, Inc. Plaintiff incorporates Exhibit “1” into his verified complaint.

COUNT I
RACKETEERING IN VIOLATION OF 18 U.S.C. § 1964

38. The operation of Defendant “1” and JOHN DOES 1-9, individually and through their alleged business in trading cryptocurrency as cryptocurrency traders in their sophisticated global internet cryptocurrency fraud and conversion scheme constitutes a racketeering operation.

39. Defendant “1” directed and coordinated with JOHN DOES 1-9 as yet unidentified additional parties (“RICO Enterprise,” or “Enterprise”) within the meaning of 18 U.S.C. § 1964(4), which Enterprise was engaged in, or the affairs of which affected, interstate and foreign commerce.

40. Defendant “1” and JOHN DOES 1-9 were each also a member of the RICO Enterprise, as each was a distinct person, separate and apart, from each of the RICO Enterprise members together.

41. The RICO Enterprise engaged in a pattern of racketeering activity.

42. Each person’s participation was effective partly because each mimicked an actual

on-going business (including the fraudulent platform Bitfract-pro.net) with a presence in the marketplace: the United States and indeed worldwide.

43. As co-conspirators, the unlawful conduct of each member of the RICO Enterprise is attributed to every member, i.e. Defendant “1” and JOHN DOES 1-9 as yet unidentified co-conspirators.

44. As set forth above, the RICO Enterprise engaged in the following predicate acts of racketeering within the meaning of 18 U.S.C. § 1961(1): Wire fraud in violation of 18 U.S.C. § 1343.

45. The predicate acts set forth in this Complaint, include defrauding Plaintiff beginning in April 2023, through domestic and international telephone communication including LinkedIn and Telegram messaging.

46. The predicate acts set forth in this Complaint are related, in that they have the same or similar purposes, results, participants, and methods of commission, and are otherwise interrelated by distinguishing characteristics and are not isolated events. The related criminal schemes set forth in this Complaint constitutes a “pattern or patterns of racketeering activity” as defined in 18 U.S.C. § 1961(5).

47. The Defendants engaged in two or more predicated acts of racketeering within a period of ten years and committed at least one such act after October 15, 1970.

48. The information that would establish further predicate acts and further acts of racketeering is solely within the control of Defendants. Plaintiff requires discovery to ferret out the further extent of predicate acts and further acts of racketeering, including the identity of similarly situated defrauded victims and the scope of the systematic fraud.

49. Defendants have received income derived, directly or indirectly, from a pattern of

rackeering activity and used or invested, directly or indirectly, part of such income, or the proceeds of such income, in acquisition of an interest in, or in the establishment or operation of, the RICO Enterprise, an enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce in violation of 18 U.S.C. § 1962(a).

50. Defendants through a pattern of rackeering activity maintain, directly or indirectly, an interest in or control of the RICO Enterprise, an enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce in violation of 18 U.S.C. § 1962(b).

51. Defendant “1” was associated with the RICO Enterprise, and conducted or participated, directly or indirectly, in the conduct of the Enterprise’s affairs through the pattern of rackeering activity described herein in violation of 18 U.S.C. § 1962(c).

52. Defendant “1” and/or JOHN DOE Defendants 1-9 as yet unidentified additional parties, each entered into a conspiracy to conduct or participate, directly or indirectly, in the conduct of the RICO Enterprises’ affairs through the pattern of rackeering activity described herein, in violation of 18 U.S.C. § 1962(d).

53. As a direct and proximate result of Defendants’ unlawful actions, Plaintiff has suffered damages.

WHEREFORE, Plaintiff STEVEN NELSON ELLER demands that judgment be entered against Defendant “1” and JOHN DOE Defendants 1-9, jointly and severally, as follows:

- (a) damages;
- (b) statutory trebled damages pursuant to 18 U.S.C. § 1964(c);
- (c) punitive damages;
- (d) costs, including reasonable attorney's fees, pursuant to 18 U.S.C. § 1964(c);

- (e) costs;
- (f) interest; and
- (g) such other and further relief as this Court deems just and proper.

COUNT II
CONVERSION

54. Through fraudulent misrepresentations, Defendants convinced Plaintiff to invest his money into cryptocurrency.

55. Defendants then convinced Plaintiff to transfer his cryptocurrency to the fake exchange owned and operated by Defendants.

56. After Plaintiff transferred his cryptocurrency assets to the fake exchange, Defendants then transferred Plaintiff's cryptocurrency to cryptocurrency addresses owned by Defendant "1" and JOHN DOE Defendants 1-9.

57. Defendants misappropriated Plaintiff's funds.

58. Defendants have converted Plaintiff's funds to their own use or to the use of others not entitled thereto and have exercised dominion and control over the funds to Plaintiff's exclusion and detriment.

59. Plaintiff has suffered damages as a direct and proximate result of Defendants' conversion.

WHEREFORE, Plaintiff STEVEN NELSON ELLER demands that judgment be entered against Defendant "1" and JOHN DOE Defendants 1-9, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

COUNT III
UNJUST ENRICHMENT

60. Plaintiff conferred a direct benefit upon Defendants by transferring the valuable

cryptocurrency that Defendants converted from Plaintiff.

61. Defendants have knowledge of the benefit Plaintiff conferred upon them and have retained such benefit.

62. The circumstances under which Plaintiff conferred, and Defendants accepted, render Defendants' retention of the benefits inequitable.

63. Equity required that Defendants return to Plaintiff the benefits he conferred upon Defendants.

WHEREFORE, Plaintiff STEVEN NELSON ELLER demands that judgment be entered against Defendant "1" and JOHN DOE Defendants 1-9, jointly and severally, for damages, interest, costs, and such other further relief as this Court deems just and proper.

COUNT IV
IMPOSITION OF CONSTRUCTIVE TRUST AND
DISGORGEMENT OF FUNDS

64. This is an action to impose a constructive trust upon the property taken from Plaintiff that is currently held by Defendants.

65. This action further calls for the restoration to Plaintiff of that wrongfully obtained property.

66. As set forth above, Defendants – through actual fraud, misappropriation, conversion, theft, or other questionable means – obtained Plaintiff's cryptocurrency, which in equity and good conscience Defendants should not be permitted to hold.

67. The cryptocurrency assets at issue are specific identifiable property and have been traced to Binance, Remitano, Btse.com, and HTX.

68. Any and all assets being held by Defendants at Binance, Remitano, Btse.com, and HTX must be held in trust for Plaintiff's benefit, and Defendants are not entitled to the benefit of wrongfully misappropriated, converted and stolen cryptocurrency assets that were taken from

Plaintiff.

69. The digital assets identified herein which are being held by Defendants at Binance, Remitano, Btse.com, and HTX must be disgorged to Plaintiff's benefit, as Defendants are not entitled to the benefit of wrongfully misappropriated, converted, and stolen cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff STEVEN NELSON ELLER demands the equitable imposition of a constructive trust over the property taken from Plaintiff that is currently under the control of Defendant "1" and/or JOHN DOE Defendants 1-9, in the identified cryptocurrency wallet addresses held at Binance, Remitano, Btse.com, and HTX and further demands that the wrongfully obtained property be returned to Plaintiff.

COUNT V
CONSPIRACY

70. The Defendants conspired and confederated with each other to commit, and committed, Conversion (Count II); and Unjust Enrichment (Count III).

71. Relying on the false statements made by Defendant "1", including that she was an expert in cryptocurrency investments, Plaintiff transferred his cryptocurrency assets to fake cryptocurrency platforms which were in actuality deposit addresses owned by JOHN DOE Defendants 1-9.

72. Defendants conspired with others via the fraudulent website Bitfract-pro.net and Telegram where they communicated with Plaintiff. Defendant "1" and JOHN DOE Defendants 1-9 are the owners of the cryptocurrency deposit addresses where Plaintiff's stolen cryptocurrency was transferred.

73. As a result, Plaintiff has suffered damages as a direct and proximate result of Defendants' conspiracy.

WHEREFORE, Plaintiff STEVEN NELSON ELLER demands that judgment be entered against Defendant "1" and JOHN DOE Defendants 1-9, jointly and severally, for damages, interest, costs, and such other and further relief as this Court deems just and proper.

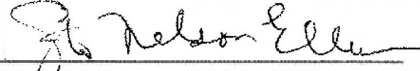
DEMAND FOR A JURY TRIAL

Plaintiff demands trial by jury on all issues so triable.

VERIFICATION

I, STEVEN NELSON ELLER, hereby declare under penalty of perjury that I have read the foregoing COMPLAINT FOR CONVERSION OF STOLEN CRYPTOCURRENCY and verify under penalty of perjury that all statements made herein are true and correct to the best of my knowledge, understanding, and belief.

Dated: August 01, 2024



Steven Nelson Eller, Plaintiff

Dated: August 1, 2024

Respectfully Submitted,

Esq. Jason S. Rathod, Esq.

Jason S. Rathod, Esq.

Nicholas A. Migliaccio, Esq.

MIGLIACCIO AND RATHOD LLP

412 H Street NE, Ste. 302

Washington, DC 20002

Telephone: 202-470-3520

Facsimile: 202-800-2730

jrathod@classlawdc.com

nmigliaccio@classlawdc.com

Attorneys for Plaintiff